Exhibit B

Michele Mair

From: Bob Reardon
Sent: Thursday, January 14, 2016 1:37 PM
To: Michele Mair
Subject: FW: Summary of Chris Grupe Unauthorized Access and Changes, and attachments

Importance: High

Micki,

Please investigate this and open a case report. Sgt Frank Johnson is going to send you an email with additional info on this subject i.e. linked in FB etc. Sounds like Grupe is in the military (a major having to do w/ IT – let's talk later as you can reach out to his Military commander as an option for leverage?)

Ricardo Karel has the computer in Mpls. To get a better understanding reach out to Thomas Gurney.

Simply, you need to verify his authority/access was shut down prior to him being terminated. (I was told it was) Sounds like he used Cached files on his laptop to do his tampering which was not retrieved when he terminated. Dig in the Mn statutes to see if there is anything in applicable for charges. When you have a grasp of this case and because this occurred in Mpls (our network is in Mpls) see who Mpls Pd IT crimes person is and meet with them in person (not over phone) & go over your file to see if there is enough to charge Grupe.

If you need to adjust your hours to work on this during the day let me know and you will be approved for it...work this case as a priority please.

Thanks,

Bob

Robert J. Reardon, Jr | Staff Sergeant | 1010 Shop Road, St. Paul MN 55106
O 651 495 9525 F 651 495 9540 | CP Police Service
24/7 Police Control Center 1 800 716 9132
www.cppoliceservice.com

From: Todd Law
Sent: Wednesday, January 13, 2016 12:56 PM
To: Bob Reardon
Subject: FW: Summary of Chris Grupe Unauthorized Access and Changes, and attachments

Bob,

Sending this email string too in case it includes something the other doesn't.

Todd

From: Bobby Walker
Sent: Wednesday, January 13, 2016 12:39 PM
To: Todd Law
Subject: FW: Summary of Chris Grupe Unauthorized Access and Changes, and attachments

Let's discuss.

Bobby A. Walker | Deputy Chief - U.S. Operations | 11306 Franklin Avenue, Franklin Park, IL 60131
O 630 860 4884|CP Police Service
24/7 Police Control Center 1 800 716 9132
www.cppoliceservice.com

. .om: Al Sauve
Sent: Wednesday, January 13, 2016 12:32 PM
To: Bobby Walker
Subject: FW: Summary of Chris Grupe Unauthorized Access and Changes, and attachments

Al Sauve, M.O.M.
Deputy Chief, Operations - Canada
Bldg 14 - 2881 Alyth Road, Calgary, Alberta T2G 5S3
Direct - 780-292-1439 | CP Police Service

24/7 Police Control Centre 1 800 716 9132
www.cppoliceservice.com

From: Mike Redeker
Sent: Wednesday, January 13, 2016 9:34 AM
To: Al Sauve
Cc: Laird Pitz; Frank Johnson; Ken Marchant
Subject: RE: Summary of Chris Grupe Unauthorized Access and Changes, and attachments

Thank you.

ıvıke Redeker
VP and CIO
Canadian Pacific
Office 403 319 6772
Cell 403 919 9487

From: Al Sauve
Sent: Wednesday, January 13, 2016 9:33 AM
To: Mike Redeker <Mike_Redeker@cpr.ca>
Cc: Laird Pitz <Laird_Pitz@cpr.ca>; Frank Johnson <Frank_Johnson@cppoliceservice.com>; Ken Marchant <Ken_Marchant@cppoliceservice.com>; Al Sauve <Al_Sauve@cppoliceservice.com>
Subject: FW: Summary of Chris Grupe Unauthorized Access and Changes, and attachments

Mr. Redeker, please be advised that Staff Sergeant Frank Johnson has been tasked with evaluating this file from a criminal perspective and overseeing any such investigation if required. You can expect to hear from him shortly.

Let me know if you have any questions or concerns....Al

Al Sauve, M.O.M.
Deputy Chief, Operations - Canada
Bldg 14 - 2881 Alyth Road, Calgary, Alberta T2G 5S3
.ct - 780-292-1439 | CP Police Service

24/7 Police Control Centre 1 800 716 9132
www.cppoliceservice.com

From: Laird Pitz
Sent: Wednesday, January 13, 2016 8:53 AM
' Al Sauve
..bject: FW: Summary of Chris Grupe Unauthorized Access and Changes, and attachments

Please review and then discuss with me. Complex to a degree ....

From: Mike Redeker
Sent: Monday, January 11, 2016 6:58 PM
To: Laird Pitz
Subject: FW: Summary of Chris Grupe Unauthorized Access and Changes, and attachments

Sir I came looking for you again today but not much luck. I would like to chat tomorrow if you have some time.

On Dec 15th we let go of an employee for poor performance but when we let him go he was remote. (I have some clean up work on how this was handled). The manager handling the employee did not take his laptop nor his aruba equipment (network connection gear) that folks remotely use to connect to the office. So while we terminated his employment we did not take away his equipment until Dec 17th when one of the leaders in IS met with him to gather the equipment. However between the time he was terminated and the time we retrieved the equipment the individual hacked into the network connection gear and proceeded to connect into CP's network. This was all completed on the morning of the 17th.

The former employee, Chris Grupe, proceeded to make his way through our network and changed key passwords in our production environment such that no one employed at CP could access mission critical networking equipment. Attached are the logs which show us Chris did the work remotely with his existing equipment and used is ~vn ID. I would like to chat with you as I believe this is a criminal activity that requires your teams support.

Please let me know if you have time tomorrow or if you would like me to reach out to someone else on your team to deal with this issue. Thanks Laird.

Mike Redeker
VP and CIO
Canadian Pacific
Office 403 319 6772
Cell 403 919 9487

From: Tim Winn
Sent: Monday, January 11, 2016 5:08 PM
To: Mike Redeker <Mike_Redeker@cpr.ca>
Subject: Summary of Chris Grupe Unauthorized Access and Changes, and attachments

Hello Mike,

Please find below Ernest's review of the log files and Crowdstrike data, identifying what it was that Chris Grupe was doing on December 17th on each of the network devices that he accessed. In some cases it was only to pull a copy of the configurations. In other cases he went much further, changing the password on the Nexus switch (which you knew about) and attempting to clear evidence of his activity. Copies of all of the log files that were pulled from the devices that Chris accessed are in the attached email. If anyone requires additional information on this, please let me or Ernest ›w.

Regards,
Tim

ı **Winn** | Sr. Director - Network Services | 7550 Ogden Dale Road SE Calgary AB T2C 4X9
O 403 319 4867 | C 403 850 7767 CP

From: Ernest Seguin
Sent: January 11, 2016 3:44 PM
To: Tim Winn
Subject: Chris Grupe Unauthorized Access and Changes

Chris Grupe used his RAP, PC and cached credentials to login into the CP network under the acct GRU0040. He did so the day after he resigned his position at CP.
He access the following Network Core Switches. I have indicated in blue log records taken from the switches. In red are the comments describing the activity.
Comments in Green are taken from the logs of the Falcon event software monitoring activities on his PC
As indicated below

Timestamp	Source	PID	ComputerName		User Name	File Name	MD5
12/17/2015 2:01:02	Falcon Host	176	7SCZH12	10.0.0.105	LOCAL SYSTEM	wininit.exe	
12/17/2015 12:01:02	Falcon Host	1196	7SCZH12	10.0.0.105	LOCAL SYSTEM	winlogon.exe	
12/17/2015 12:01:07	Falcon Host						
12/17/2015 12:01:08	Falcon Host						
12/17/2015 12:01:15	Falcon Host	7128	7SCZH12	10.0.0.105	gru0040	taskeng.exe	65ea57712340c09b1b0c427b4848a
*12/17/2015 12:02:07	Falcon Host	7624	7SCZH12	10.0.0.105	gru0040	ipconfig.exe	cf45949cdbb39c953331cdcb9cec20
12/17/2015 12:02:48	Falcon Host	5772	7SCZH12	10.0.0.105	gru0040	kitty.exe	2deb785e7382402d8cc2c7f31d4ecl

(* Above is Grupe logging into CP after his resignation and using SSH to access the network gear *)
==============
copnx7sw01 (* This is the Ogden Core Switch that controls and directs all Data Center traffic for critical corporate and in control applications *)

Thu Dec 17 05:35:07 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:35:26 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:35:26 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:35:37 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=copy running-config tftp:/ (FAILURE)
J Dec 17 05:36:22 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:41:15 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:41:16 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:41:25 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:41:51 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:41:51 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:42:01 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:42:08 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:43:26 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:43:26 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:43:43 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=copy running-config tftp:/ (FAILURE)
(* Above he tried and failed twice to copy off the CP private configuration *)
Thu Dec 17 05:43:57 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=ping 10.188.206.220 (SUCCESS)
Thu Dec 17 05:46:06 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted user cpadmin
Thu Dec 17 05:46:06 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted v3 user : cpadmin
Thu Dec 17 05:46:06 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=configure terminal ; no username cpadmin (SUCCESS)
Thu Dec 17 05:46:10 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted user arcnsparc
Thu Dec 17 05:46:10 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted v3 user : arcnsparc
Thu Dec 17 05:46:10 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=configure terminal ; no username arcnsparc (SUCCESS)
(* Above he removed successfully two device administration accounts *)
J Dec 17 05:49:26 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=clear logging logfile (SUCCESS)
Thu Dec 17 05:49:32 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=clear logging nvram (SUCCESS)
(* Above he removed all evidence of his activity from the active memory log, but this does not remove all log info *)
Thu Dec 17 05:52:52 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=Performing configuration copy.
Thu Dec 17 05:52:53 2015:type=start:id=vsh.24445:user=root:cmd=
Thu Dec 17 05:52:53 2015:type=stop:id=vsh.24445:user=root:cmd=
Thu Dec 17 05:53:05 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=copy running-config startup-config (SUCCESS)
Thu Dec 17 05:53:11 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:53:11 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=
(* Above he did successfully copy off the CP crticial config DATA*)
Thu Dec 17 06:37:34 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc cppcorsw01 (SUCCESS)
Thu Dec 17 06:52:17 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc cppdstsw01 (SUCCESS)
(*Above he successfully removed the last critical admin account and now the switch no longer could be controlled or managed by authorized CP network staff or anyone but him *)
(* At this point the railway was at extreme risk. He left all the monitoring only rights in place so that the system would appear normal *)
(* If an emergency communication problem occurred, CP staff would not be able to fix it *)
Thu Dec 17 06:52:20 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=shell terminated gracefully
(* He then signed out *)

===============
cppnx7sw02

Thu Dec 17 06:07:57 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc cppdcisw02 (SUCCESS)
Thu Dec 17 06:52:24 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc cppcorsw02 CCESS)
Thu Dec 17 06:52:39 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=dir bootflash:/ (SUCCESS)
Thu Dec 17 06:52:55 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=shell terminated gracefully
(* Above he logged into the second core switch at the Ogden data center and was poking around *)

===============
(* Below he logged into the core switch at CPP *)
cppcorsw01

Thu Dec 17 05:59:15 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:59:47 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 05:59:47 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 06:00:08 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto ; copy running-config tftp:/ (SUCCESS)
(* Above he successfully took a copy of the CP private configuration on the box. *)
Thu Dec 17 06:09:43 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 06:09:44 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 06:10:08 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted user cprailMain
Thu Dec 17 06:10:08 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted v3 user : cprailMain
Thu Dec 17 06:10:08 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto ; configure terminal ; no username cprailMain (SUCCESS)
(* Above he removed most, but not all administration accounts *)
u Dec 17 06:10:14 2015:type=start:id=vsh.25870:user=root:cmd=
Thu Dec 17 06:10:15 2015:type=stop:id=vsh.25870:user=root:cmd=
Thu Dec 17 06:10:25 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto ; copy running-config startup-config (SUCCESS)
(* Here he saved his current changes permanently *)
Thu Dec 17 06:10:49 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 06:13:46 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 06:13:46 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 06:15:16 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 06:15:47 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 06:15:47 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 06:37:34 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=shell terminated gracefully
(* Here he exists the site *)

================
(* Below he logs into the second core switch at CPP alternate data center *)
cppcorsw02

Thu Dec 17 06:08:05 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 06:08:19 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 06:08:19 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=

Thu Dec 17 06:08:40 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto ; copy running-config tftp:/ (SUCCESS)
(* Above he successfully obtains copies of the CP private config *)
Thu Dec 17 06:09:22 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 06:09:22 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 06:09:54 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
ı Dec 17 06:09:54 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 06:52:24 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=shell terminated gracefully
(* He then exits *)

================

cppdstsw01
(* Below he logs into the host distribution switch at cpp *)
Thu Dec 17 05:13:27 2015:type=start:id=10.188.206.220@pts/0:user=admin:cmd=
Thu Dec 17 05:13:41 2015:type=start:id=10.188.206.220@pts/0:user=admin:cmd=
Thu Dec 17 05:13:41 2015:type=stop:id=10.188.206.220@pts/0:user=admin:cmd=
Thu Dec 17 05:13:54 2015:type=update:id=10.188.206.220@pts/0:user=admin:cmd=copy running-config tftp:/ (SUCCESS)
(* Again he copies off the CP private configs *)
Thu Dec 17 06:37:48 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 06:38:45 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto ; copy bootflash:/ tftp:/ (SUCCESS)
(* Again he copies off the CP private configs *)
Thu Dec 17 06:38:56 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto ; delete bootflash:/cppvpcbrief.txt (SUCCESS
)
(* Here he deletes a backup file *)
ı Dec 17 06:39:51 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto ; dir bootflash:/ (SUCCESS)
Thu Dec 17 06:39:55 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto ; dir bootflash:/ (SUCCESS)
(* Here he lists out all the files stored on the device flash *)
Thu Dec 17 06:41:32 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto ; copy bootflash:/ tftp:/ (SUCCESS)
(* Here he takes copy of this device CP private config *)
Thu Dec 17 06:51:41 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto ; dir bootflash:/ (SUCCESS)
Thu Dec 17 06:52:03 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto ; delete bootflash:/shintstatus.txt (SUCCESS
)
(* here he removes an interface show status txt file *)
Thu Dec 17 06:52:06 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto ; dir bootflash:/ (SUCCESS)
Thu Dec 17 06:52:17 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=shell terminated gracefully
(* Here he exits *)

(* Below is the activities on the second critical Core switch in Ogden
================
Ogncorsw02
Dec 17 09:40:42 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogncorsw02 (SUCCESS)
(* Here he switches context to the core Virtual switch. *)
Dec 17 09:40:47 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=added user:admin to the role:network-admin
Dec 17 09:40:47 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=updated v3 user : admin
: 17 09:40:47 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=configure terminal ; username admin password 0 *******

(* Above he adds a new overall administrator and sets a new password. This effectively locks out admin by anyone but himself *)

Dec 17 06:41:37 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogncorsw01 (SUCCESS)

Dec 17 09:42:05 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogncorsw02 (SUCCESS)

Dec 17 09:42:23 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogndstsw02 (SUCCESS)

Dec 17 09:44:57 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=dir bootflash:/ (SUCCESS)

17 06:45:09 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogncorsw01 (SUCCESS)

Dec 17 09:45:38 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=dir bootflash:/vdc_2/ (SUCCESS)

Dec 17 09:46:00 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=shell terminated gracefully

Dec 17 06:48:21 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogncorsw01 (SUCCESS)

Dec 17 06:48:34 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=added user:admin to the role:network-admin

Dec 17 06:48:34 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=updated v3 user : admin

Dec 17 06:48:34 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=configure terminal ; username admin password 0 *******

(* Here he changes the overall administrator for the Ogden core *)

Dec 17 06:50:42 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogndstsw01 (SUCCESS)
Dec 17 06:51:33 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=shell terminated gracefully

Summary Evaluation
Why take the configs?
Most likely to reference them at a later date if he needed too.

Why change the passwords?
Lock out the switches from administration, but allow them to function until a failure at a later date.

Why not do more?
He was likely using cached creditenials on his PC. When he connected to CP, his cached creds would be expired, but s
cess until his screen saver cut in. At this point he would be stuck and could not do more. He wiped out his disk pa
assets.

Take Care,
Ernest